12.3　バックアップ
目的：データの消失から保護するため
12.3.1　情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査する。
12.3.1.1　バックアップ方針を確立し、情報、ソフトウェア及びシステムイメージのバックアップに関する組織の要求事項を定める。
12.3.1.2　バックアップ方針では、保管及び保護に関する要求事項を定める。
12.3.1.3　災害又は媒体故障の発生の後に、全ての重要な情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備える。
12.3.1.4　バックアップ情報の正確かつ完全な記録及び文書化したデータ復旧手順を作成する。
12.3.1.5　バックアップの範囲（例えば、フルバックアップ、差分バックアップ）、及びバックアップの頻度は、組織の業務上の要求事項、関連する情報のセキュリティ要求事項、及びその情報の組織の事業継続に対しての重要度を考慮して決定する。
12.3.1.6　バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた場所に保管する。
12.3.1.7　バックアップ情報に対して、主事業所に適用されている標準と整合した、適切なレベルの物理的及び環境的保護を実施する。
12.3.1.8　バックアップに用いる媒体は、必要になった場合の緊急利用について信頼できることを確実にするために、定めに従って試験する。
12.3.1.9　バックアップに用いる媒体の試験は、データ復旧手順の試験と併せて行い、必要なデータ復旧時間に照らし合わせて確認する。
12.3.1.10　バックアップデータを復旧させる能力の試験は、バックアップ手順又はデータ復旧プロセスに失敗し、データに修復不能な損傷又は損失が発生した場合に備えて、原本の媒体に上書きするのではなく、専用の試験媒体を用いて行う。
12.3.1.11　機密性が重要な場合には、暗号化によってバックアップ情報を保護する。
12.3.1.12　運用手順では、バックアップ方針に従って、バックアップの完全性を確保するために、その実行を監視し、計画されたバックアップの失敗に対処する。
12.3.1.13　個々のシステム及びサービスに関するバックアップの取決めは、事業継続計画の要求事項を満たすことを確実にするために、定めに従って試験する。
12.3.1.14　重要なシステム及びサービスに関するバックアップの取決めは、災害に際してシステム全体を復旧させるために必要となる、システム情報、アプリケーション及びデータの全てを対象とする。
12.3.1.15　永久保存する複製物に関するあらゆる要求事項を考慮に入れて、不可欠な業務情報の保管期間を決定する。
12.4　ログ取得及び監視
目的：イベントを記録し、証拠を作成するため
12.4.1　利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。
12.4.1.1　イベントログには、利用者ＩＤを含める。
12.4.1.2　イベントログには、システムの動作を含める。
12.4.1.3　イベントログには、主要なイベントの日時及び内容（例えば、ログオン、ログオフ）を含める。
12.4.1.4　イベントログには、装置のＩＤ又は所在地（可能な場合）、及びシステムの識別子を含める。
12.4.1.5　イベントログには、システムへのアクセスの、成功及び失敗した試みの記録を含める。
12.4.1.6　イベントログには、データ及び他の資源へのアクセスの、成功及び失敗した試みの記録を含める。
12.4.1.7　イベントログには、システム構成の変更を含める。
12.4.1.8　イベントログには、特権の利用を含める。
12.4.1.9　イベントログには、システムユーティリティ及びアプリケーションの利用を含める。
12.4.1.10　イベントログには、アクセスされたファイル及びアクセスの種類を含める。
12.4.1.11　イベントログには、ネットワークアドレス及びプロトコルを含める。
12.4.1.12　イベントログには、アクセス制御システムが発した警報を含める。
12.4.1.13　イベントログには、保護システム（例えば、ウィルス対策システム、侵入検知システム）の作動及び停止を含める。
12.4.1.14　イベントログには、アプリケーションにおいて利用者が実行したトランザクションの記録を含める。
12.4.2　ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護する。
12.4.2.1　記録されたメッセージ形式の変更から保護する。
12.4.2.2　認可されていないログファイルの編集又は削除から保護する。
12.4.2.3　イベント記録の不具合又は過去のイベント記録への上書きを引き起こす、ログファイル媒体の記録容量超過の問題から保護する。
12.4.3　システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューする。
12.4.3.1　特権を与えられた利用者（システムの実務管理者及び運用担当者）に関する責任追跡性を維持するために、その作業を記録する。
12.4.3.2　特権を与えられた利用者（システムの実務管理者及び運用担当者）に関する責任追跡性を維持するために、その利用者の作業のログを保護する。
12.4.3.3　特権を与えられた利用者（システムの実務管理者及び運用担当者）に関する責任追跡性を維持するために、その作業のログを定期的にレビューする。
12.4.4　組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させる。
12.4.4.1　時刻の表示、同期及び正確さに関する外部及び内部の要求事項は、文書化する。
12.4.4.2　組織内で用いるための基準となる時刻源を定める。
12.4.4.3　基準となる時刻源を外部から取得するための組織の取組み及び内部のクロックを確実に同期させる方法を文書化し、実施する。
12.5　運用ソフトウェアの管理
目的：運用システムの完全性を確実にするため
12.5.1　運用システムに関わるソフトウェアの導入を管理するための手順を実施する。
12.5.1.1　運用ソフトウェア、アプリケーション及びプログラムライブラリの更新は、適切な管理層の認可に基づき、訓練された実務管理者だけが実施する。
12.5.1.2　運用システムは、実行可能なコードだけを保持し、開発用コード又はコンパイラは保持しない。
12.5.1.3　アプリケーション及びオペレーティングシステムソフトウェアは、十分な試験に成功した後に導入する。
12.5.1.4　アプリケーション及びオペレーティングシステムソフトウェアの試験は、使用性、セキュリティ、他システムへの影響及びユーザフレンドリー性の試験を含める。
12.5.1.5　アプリケーション及びオペレーティングシステムソフトウェアの試験は、運用システムとは別のシステムで実行する。
12.5.1.6　アプリケーション及びオペレーティングシステムソフトウェアの試験は、対応するプログラムソースライブラリが更新済みであることを確実にする仕組みを整備する。